University of Edinburgh, School of Informatics

Secure Programming Coursework: Part 1

1. RIDL and Fallout

Question 1

The term speculative execution refers to the optimization technique where a processor fulfills instructions that might be executed in the short-term future. Ultimately, the incorrectly executed code will be reverted afterward.

When the CPU speculatively executes an instruction doesn't understand that this should not happen. Hence, data might be loaded into the cache memory. Afterward, the attacker uses a covert side-channel (usually timing attacks) to recover the private data from the cache memory.

Meltdown and Spectre are the defacto attacks leveraging speculative execution to leak information. Researchers recently discovered two other attacks that exploit the same optimization techniques. RIDL and Fallout vulnerabilities, also known as "Microarchitectural Data Sampling", leak information from other CPU components. Precisely, the RIDL attack concerns "fill buffers", "load ports", and the "memory controller". Likewise, Fallout relates to CPU "store buffers". Intel's implementation of simultaneous multithreading (Hyperthreads) allows threads to share the same buffers and data. Hence, a malicious thread can access the data of another thread, that use the same CPU components.

Meltdown, Spectre, RIDL, and Fallout might have some similarities, but they are essentially different. Meltdown and Spectre operate on the cache level, while RIDL and Fallout operate on processors buffers. We find RIDL and Fallout on Intel CPUs only that use Hyperthreading. However, Meltdown and Spectre are common problems for Intel, AMD, and ARM processors. We can fix the RIDL attack by disabling Hyperthreading. Also, there was a patch for the Fallout attack by partitioning the buffer, so each thread accesses only a part of it. On the other hand, there is no way to fix Meltdown and Spectre vulnerabilities unless you change your hardware.

Question 2

- **RIDL:** CVE-2018-12130 CVE-2018-12127, CVE-2019-11091
- **Fallout:** CVE-2018-12126

Question 3

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Confidentiality is violated because an adversary might expose the user's private data.

Question 4

The attacker using RIDL and Fallout attacks can read arbitrary data values, which leads to loss of confidentiality. Generally, the attacker might gain access to personal messages, health records, financial data, secret passwords, and many more. The consequences of losing confidentiality are correlated to the loss of privacy. This can cause emotional damage (public embarrassment or reputational effects), loss of autonomy/freedom, trust, and harm a person/entity financially.

Question 5

To distinguish software and hardware vulnerabilities, we answer the following four questions:

- *Who can fix it?*

Usually, hardware vulnerabilities can be fixed by hardware manufacturers that employ technical staff who deeply understand the blueprints of their circuits. Sometimes OS developers can handle some issues at the kernel level, but this is not always the case. On the other hand, almost anyone with a good programming understanding can fix software vulnerabilities, especially if the software is open-source so that anyone can access its source code.

- *How fast can we patch it?*

Usually, software vulnerabilities are much faster to patch. Instead, hardware issues are much more complex and slower to repair.

- *Is the vulnerability immediately exploitable?*

Software vulnerabilities can be more easily exploited since the attackers know the software attack surface better. Anyone with good programming skills can initiate a software attack. On the other hand, hardware attacks are much more sophisticated and require niche skills, making the attackers unable to exploit them directly.

- *From an economic perspective, is it efficient to fix it?*

From an economic point of view, resolving hardware vulnerabilities requires replacing the hardware with a financial overhead. In some cases, like smartphone hardware, manufacturers won't bother fixing the phones because people buy new phones very frequently. Besides that, securing hardware comes with performance tradeoffs. For instance, if a cloud provider fixes its servers might face performance issues that will cost millions of dollars to the company.

Examples:

- Hardware vulnerability: CVE-2020-8694 https://nvd.nist.gov/vuln/detail/CVE-2020-8694
- Software vulnerability:CVE-2021-41817 https://nvd.nist.gov/vuln/detail/CVE-2021-41817

Question 6

Mr. Super Secure's computer is not safe. Scanning a computer for malicious programs or installing a firewall might slow down the attackers, but it might not stop them eventually. Specifically, we are more concerned about a chain of zero-day attacks that might allow the adversary to bypass the firewall and dig into Mr. Super Secure's system. At this point, the attacker might exploit the hardware vulnerabilities. Besides that, hardware attacks are possible even if the machines are not connected to the same network. For example, consider virtual machines on a cloud platform. Any virtual machine on the platform which operates on the same host could leverage RIDL or Fallout to attack the virtual machine that uses the same hardware. Hence, a firewall or an Antivirus can not protect him. The only way to secure a system is to get a new, non-vulnerable processor.

Quetion 7

Measures to mitigate RIDL and Fallout attacks:

- Disable Hyperthreading on your processor (you have to sacrifice performance)
- Replace your processor with a new one that is non-vulnerable (ARM and AMD processors are not vulnerable for the moment)